ABSTRACT

Disclosed is a method for authenticating a mobile node in a wireless local area network including at least two access points and an authentication server. When the mobile node associates with a first access point and performs initial authentication, the mobile node receives a first session key for secure communication from the authentication server by using a first private key generated with a secret previously shared with the authentication server, and the first access point receives the first session key from the authentication server by using a second private key previously shared with the authentication server. When the mobile node is handed over from the first access point to a second access point and performs re-authentication, the mobile node receives a second session key for secure communication from the authentication server by using a third private key generated with authentication information generated during previous authentication and shared with the authentication server and the second access point receives the second session key from the authentication server by using the second private key previously shared with the authentication server.